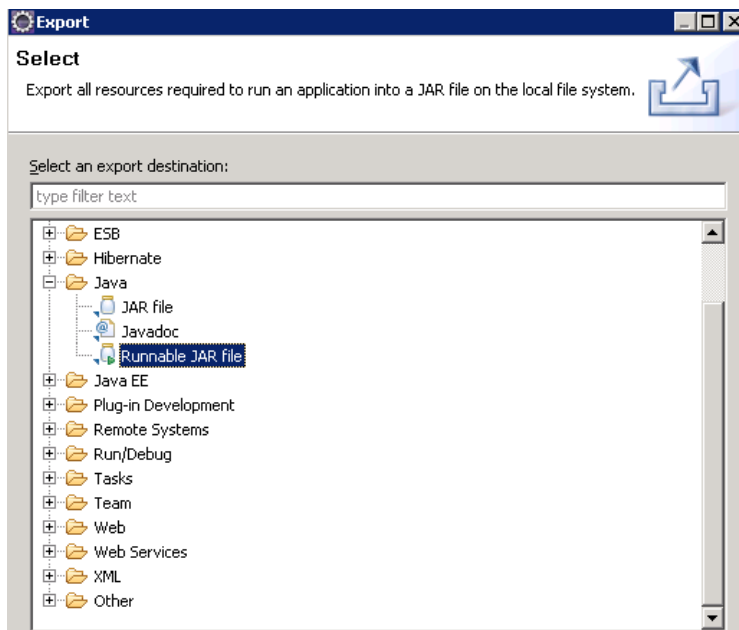


Práctica: Políticas de seguridad a partir de código firmado

Objetivo: Generar claves privadas, firmas código java y establecer políticas de seguridad

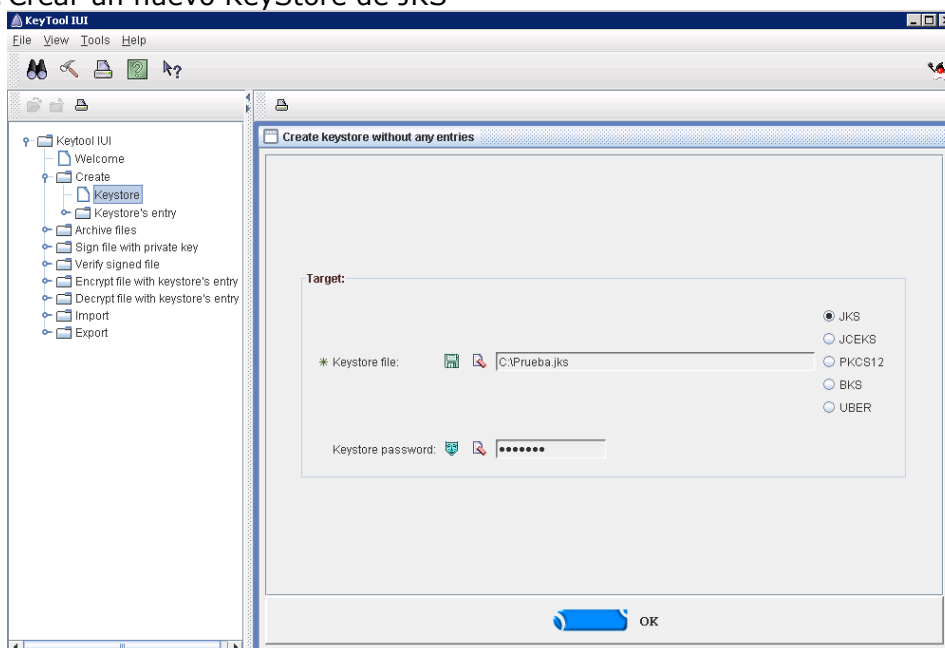
Desarrollo:

1. Exportar la aplicación a formato JAR

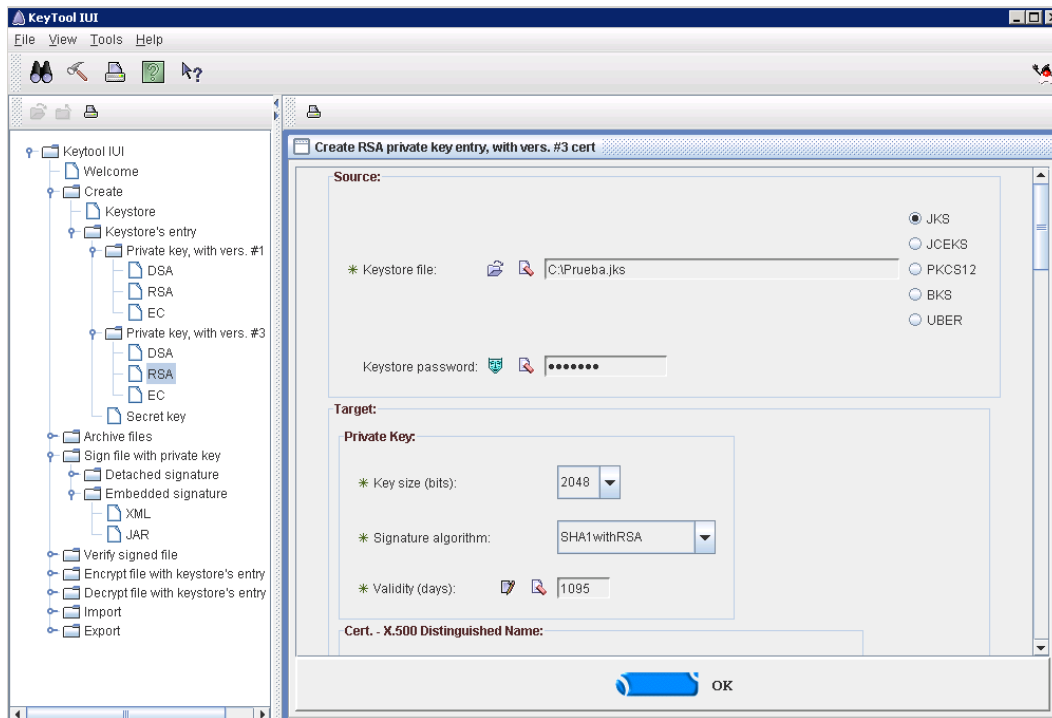


2. Arrancar la aplicación KeyTool IUI, una interfaz gráfica para keytool

2.1. Crear un nuevo KeyStore de JKS



- 2.2. Crear una clave privada V3 utilizando el keystore previamente definido, el algoritmo utilizado para la firma será SHA1 con RSA, escribir como common name CN=ATOS.COM, y comprobar que el propósito de firma digital está activado



2.3. Introducir un alias y una clave la clave creada

Enter new private key entry's alias: atos

Enter new password: *****

Confirm new password: *****

OK CANCEL

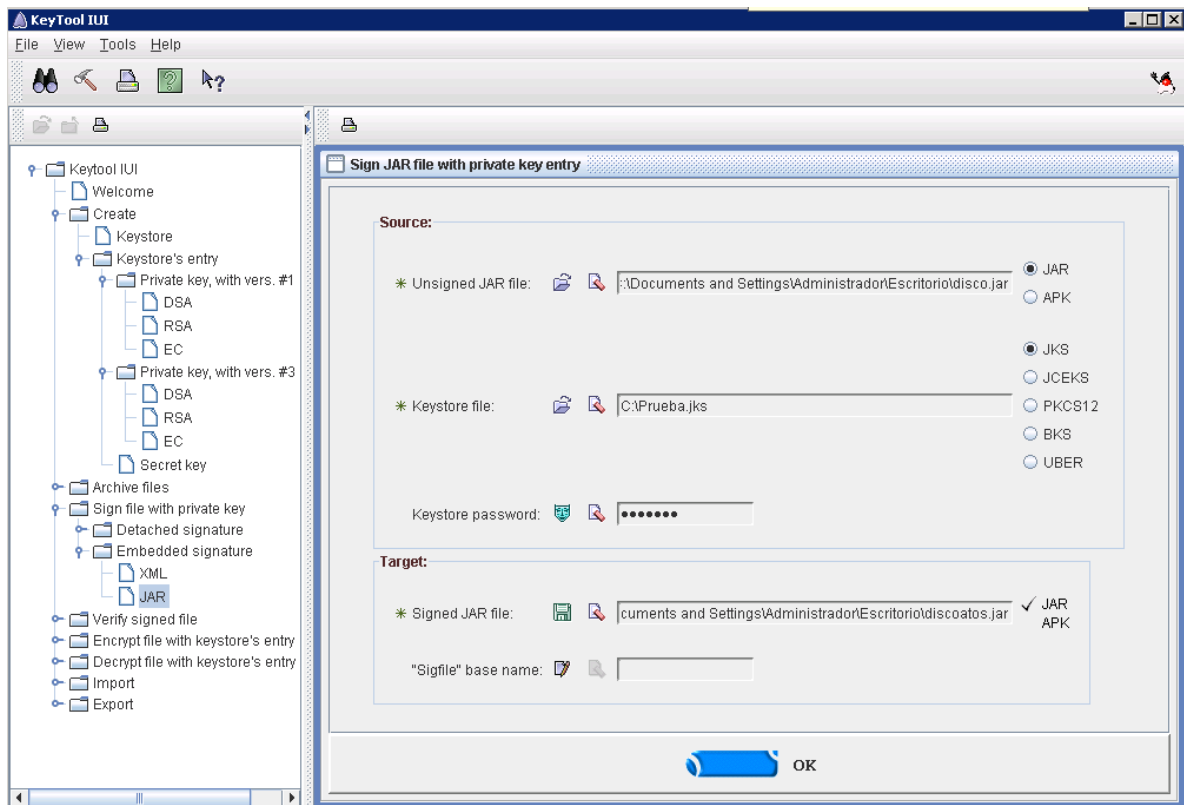
2.4. El certificado aparecerá en el almacén

KeyTool IUI - JKS keystore manager

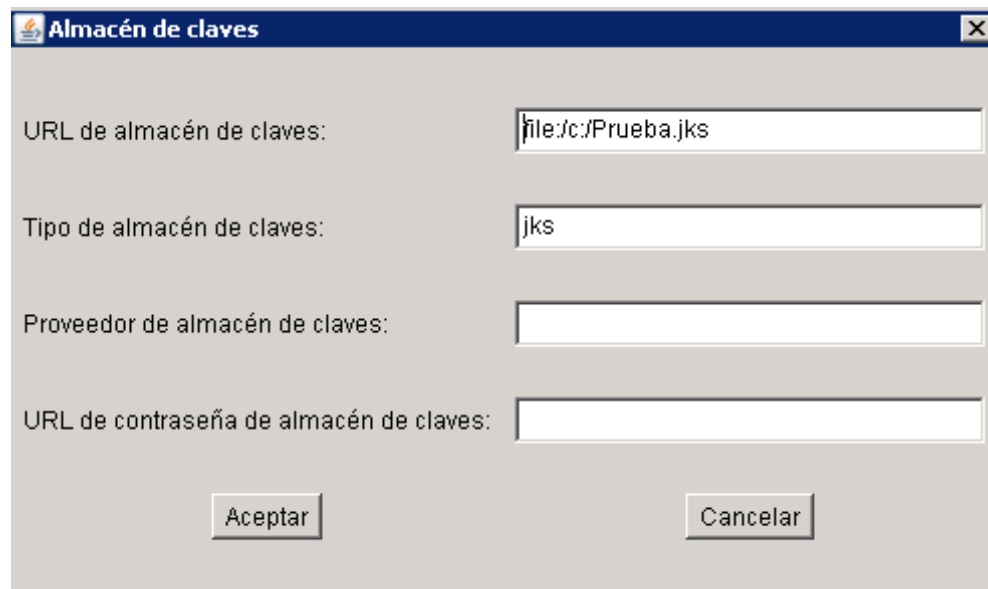
Private Key (keypair) & Trusted Certificate Entries:

Alias	Entry	Valid Date ?	Self-Signed ?	Trusted C.A. ?	Key Size	Cert. Type	Cert. Sig. Algo.	Modified Date
atos		✓	✓	-	2048 bits	X.509	SHA1withRSA	04-jun-2013

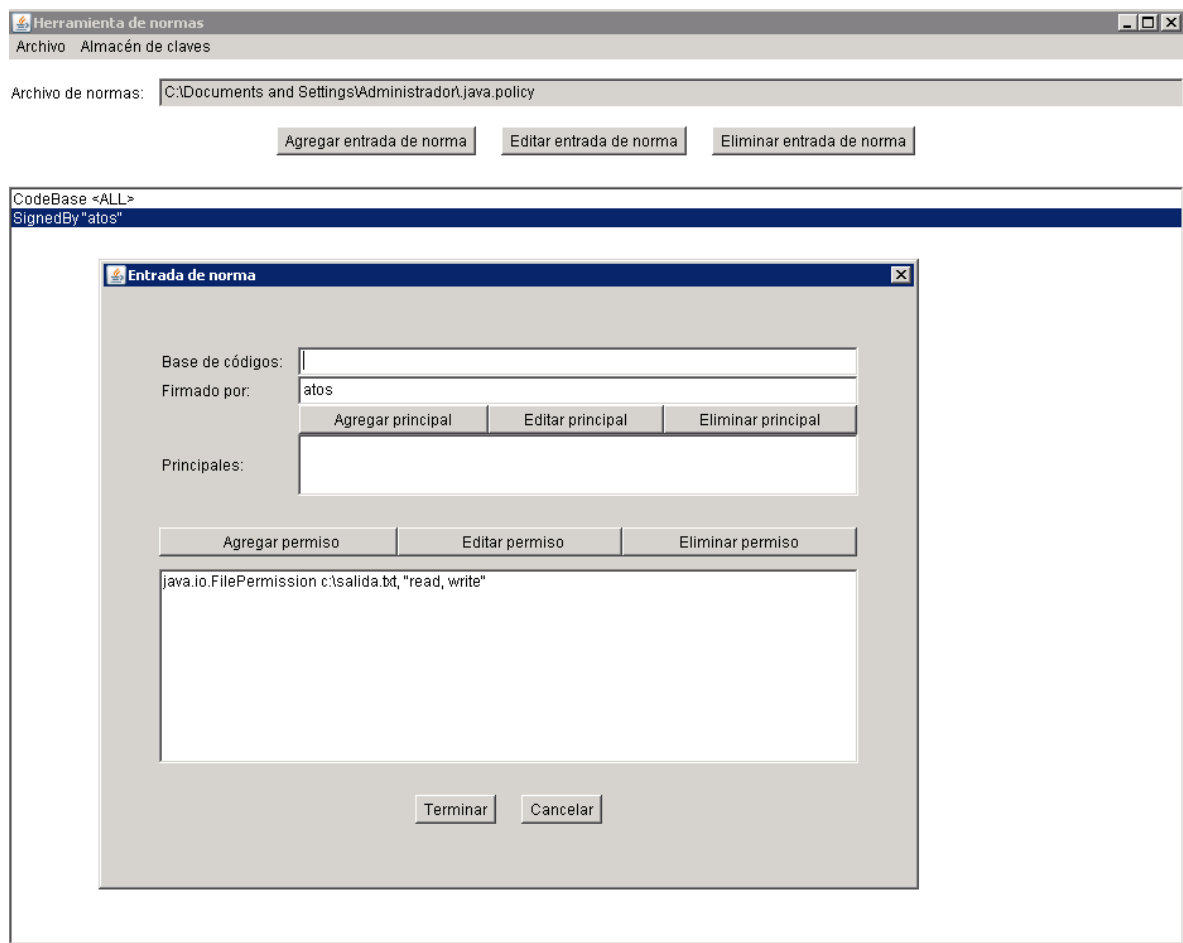
2.5. Firmar el jar con la clave privada generada, embebiendo la firma en el JAR y verifica si se encuentra firmada



Abrir la herramienta policytool y configura el almacén de claves



3. Configura la política de seguridad para dar permisos al código firmado por la clave privada "atos":



Herramienta de normas

Archivo Almacén de claves

Archivo de normas: C:\Documents and Settings\Administrador\java.policy

Agregar entrada de norma Editar entrada de norma Eliminar entrada de norma

CodeBase <ALL>
SignedBy "atos"

Entrada de norma

Base de códigos:

Firmado por: atos

Agregar principal Editar principal Eliminar principal

Principales:

Agregar permiso Editar permiso Eliminar permiso

java.io.FilePermission c:\salida.bt, "read, write"

Terminar Cancelar